



DEPARTMENT OF THE ARMY  
HEADQUARTERS, 34TH DIVISION (INSTITUTIONAL TRAINING)  
4020 W. SILVER SPRING DRIVE  
MILWAUKEE, WISCONSIN 53218-3494

REPLY TO  
ATTENTION OF

14 September 2002

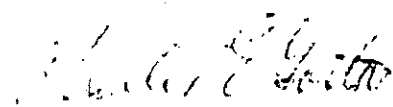
MEMORANDUM FOR SPC David R. Olofson, 392- [REDACTED] N7155 Winnebago Drive, Fond du Lac, WI 54935

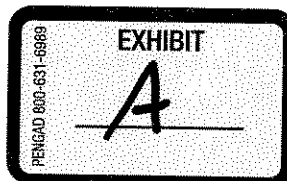
SUBJECT: General Officer Memorandum of Reprimand

1. Background. You were assigned to the 2/274 Battalion from May 2001 to May 2002. During that period, you worked in the personnel section as a Personnel Administration Specialist. Your duties required you to have access to the computers located at the Fond du Lac Reserve Center. Full-time personnel also granted you access to the Intranet and the Internet. With your access, you reconfigured the center's information management systems. Additionally, you integrated your own personal computer systems into the Government systems. You downloaded restricted files and established unauthorized nets. When personnel began investigating the unauthorized changes, you destroyed security logs, removed drives, and deleted files. Your actions violated Army regulations regarding security and USARC information management policies.
2. Reprimand. I reprimand you for your abysmal failure to adhere to basic security measures. Your age and experience in the information management field make your actions all the more reprehensible and inexcusable. Your demonstrated lack of respect for Army regulations and policies indicates a basic incompatibility with military service. Your deplorable conduct is wholly unacceptable and intolerable in a senior soldier.
3. Administrative Action. This reprimand is administrative in nature and is not imposed as punishment under the provisions of the Uniform Code of Military Justice.
4. Filing. I intend to place this memorandum in the performance fiche portion of your Official Military Personnel File (OMPF). I am referring this memorandum to you for comment because it contains derogatory information. You will reply by memorandum (sample enclosed) to me no later than ten days from receipt of this letter. You may include comments and information regarding matters in extenuation or mitigation. I will consider any timely submissions before deciding whether to make this letter of reprimand final and the appropriate location for filing.

2 Encls

1. AR 15-6 Investigation excerpt
2. Sample Memorandum

  
CHARLES E. GORTON  
Major General, USAR  
Commanding





DEPARTMENT OF THE ARMY  
HEADQUARTERS, 4TH DIVISION (INSTITUTIONAL TRAINING)  
4828 W. SILVER SPRING DRIVE  
MILWAUKEE, WISCONSIN 53218-3488

REPLY TO  
ATTENTION OF


29 November 2012

MEMORANDUM FOR Commander, U.S. Army Reserve Personnel Command, ATTN: AIPC-  
ZJA, 1 Reserve Way, St. Louis, MO 63132-5200

SUBJECT: Filing of General Officer Memorandum of Reprimand for SPC David R. Olofson,  
[REDACTED]

1. Consideration of Rebuttal. I fully considered the facts concerning my enclosed Memorandum of Reprimand. I also considered the soldier's lack of acceptance of my memorandum (delivery attempted on 18 and 23 September, and 03 October 2002 (see enclosure)).
2. Filing. I direct the enclosed Memorandum of Reprimand be filed permanently in the performance fiche portion of his Official Military Personnel File and in his Military Personnel Records Jacket.

Encl  
as

  
CHARLES E. GORTON  
Major General, USAR  
Commanding

CF:  
SPC Olofson  
CDR, 2274<sup>th</sup> BN  
CDR, 2<sup>nd</sup> Bde

#### SECTION IV - FINDINGS

1. Who authorized 2/274<sup>th</sup> personnel to modify ADP systems? SFC [REDACTED] authorized SPC David R. Olofson to make modifications to ADP systems. These modifications were not in accordance with Department of the Army or USARC regulations. No one authorized [REDACTED] to modify or allow modifications to the ADP equipment. The modifications violated 18 USC 1030: Wrongful Damage of a Government Computer, AR 380-5, AR 380-1, AR 380-19, USARC Memorandum 25-70, and USARC Memorandum 380-1. Based on statements by the commander, LTC Ricks, and SFC Hyton, there was a lack of supervision by [REDACTED] Unit Administrator, of [REDACTED]. No full time personnel tried to find out what [REDACTED] or SPC Olofson was doing, check regulations, or question the additional network systems.

LTC Ricks on 5 May 2002 became aware that [REDACTED] and SPC Olofson may have modified military government equipment, established an unauthorized network, and permitted civilians and/or civilian organizations access to military information. He immediately ordered [REDACTED] to keep SPC Olofson out of the unit and away from military ADP equipment. The next day, 6 May 2002, [REDACTED] allowed SPC Olofson into the Reserve Center. The two spent between five and six hours working on military government equipment. It can be inferred that [REDACTED] and SPC Olofson were responsible for what the Information Management team found the following day, 7 May 2002. The Information Management directorate of 84<sup>th</sup> Division arrived and confirmed the unauthorized network. Additionally, the IM team indicated that drives were removed, files deleted, equipment removed, and security logs were blank. (Exhibits 1, 2, 9, 11, 13, 20)

2. If authorized to make modifications, what was the scope of the modifications? [REDACTED] and SPC Olofson used SPC Olofson's personal computer equipment in conjunction with ADP systems and Government phone lines. They were not authorized to do so; however, the commander, LTC Ricks, approved an AAM for SPC Olofson for "donating numerous personal resources in the process of maintaining Battalion-wide data processing equipment." This was in violation of DA and USARC regulations. (Exhibits 1, 2, 13, 19)

3. Who authorized 2/274<sup>th</sup> personnel to use personal computer equipment in conjunction with ADP systems and Government phone lines? [REDACTED] improperly authorized SPC Olofson to connect his personal computers to government systems. [REDACTED] was aware but took no action to prevent this. [REDACTED] and SPC Olofson created a private network that circumvented government network by connecting SPC Olofson's personal computer to government computers, and by using another personal computer as a server. [REDACTED] and SPC Olofson violated 18 USC 1030: Unauthorized Access To A Government Computer, 18 USC 1030: Wrongful Damage Of A Government Computer, 18 USC 371: Conspiracy, the Privacy Act, AR 380-5, AR 380-1, AR 380-19, USARC Memorandum 25-70, USARC Memorandum 380-1. (Exhibits 1, 2, 6, 9, 11, 10)

4. What modifications were made to ADP systems? What were the apparent purpose of any modifications made to ADP systems? SFC [REDACTED] and SPC Olofson spent five hours altering the computer systems, removing files, erasing disks, so it is not possible at this time to say what the exact modifications were. The apparent purposes of the modifications were: to improve the performance of the government systems, to access:

soldier personnel information such as Social Security Numbers, NCOERs, training schedules, unit rosters, and to be able to use the Internet. (Exhibits 1, 2, 5, 9, 13, 20)

5. Who made any modifications to ADP systems? Only SFC [REDACTED] and SPC Olofson had the passwords necessary to make modifications. Therefore, it can be inferred that SFC [REDACTED] and SPC Olofson made the modifications. (Exhibits 5, 8, 9, 11, 20)

6. If modifications were made, did the modifications violate Army regulations and/or policies? The modifications violated 18 USC 1030: Wrongful Damage of a Government Computer, AR 380-5, AR 380-1, AR 380-19, USARC Memorandum 25-70, and USARC Memorandum 380-1.

Additionally, they violated 18 USC 371: Conspiracy. SFC [REDACTED] and SPC Olofson took several inappropriate actions before and after discovery of the modifications. They downloaded on personal computers soldiers' personal information in violation of the Privacy Act. They networked systems without permissions. They permitted sensitive information to be vulnerable to hackers and other cyber security threats. SPC Olofson told several soldiers that he downloaded all unit information onto his personal computer at the end of each drill. SFC [REDACTED] and SPC Olofson may have permitted Wisconsin militia group(s) to access the Internet through military IP addresses. (Exhibits 1, 2, 11)

7. What actions were taken by the Battalion Commander upon notification of inappropriate behavior of 2/274<sup>th</sup> personnel that highlighted personal safety issues? What inappropriate actions were taken by 2/274<sup>th</sup> personnel pursuant to discovery by higher commands of possible modifications made to ADP systems? Did full-time staff members of the 2/274<sup>th</sup> violate direct orders regarding ADP systems? Once notified of the improper networked systems, LTC Ricks ordered SFC [REDACTED] to keep SPC Olofson out of the unit center. LTC Ricks called the IM to investigate. At a later date, he drove to SPC Olofson's home and gave him a counseling statement informing him that he could not return to the center. LTC Ricks did not tell the UA or other full time personnel of his orders to SFC [REDACTED]. SFC [REDACTED] disobeyed LTC Ricks order by permitting SPC Olofson into the center and access to military ADP systems. After the incidents were discovered and SFC [REDACTED] was ordered to not let SPC Olofson into the center, SFC [REDACTED] directly disobeyed LTC Ricks and permitted SPC Olofson 5-6 hours to modify equipment, remove zip drives and files, remove personal equipment, erase information, destroy a drive, and commit possible other damage. Additionally, the center's back door was found propped open by either SPC Olofson or SFC [REDACTED]. Mr. Schubert locked the door, so no more criminal activities took place. (Exhibits 9, 11, 14, 20)

8. Did 2/274<sup>th</sup> personnel engage in inappropriate and/or unlawful activity that encouraged other individuals to engage in activities that violate state and/or federal law? There is no evidence to show that others were encouraged to or involved in violating state and/or federal laws.

#### Additional findings

9. SFC [REDACTED] made false statements to the IM team in front of SFC Hylton and Mr. Schubert during the team's investigation. He said that the only personal equipment SPC Olofson used was a palm pilot. He did not tell about the personal computer of SPC Olofson that was used as a server. (Exhibits 1, 2, 9, 11, 13)

10. SPC Olofson has been found guilty of carrying concealed weapons. He has never informed the Army of his convictions. He presently has several other charges pending for carrying concealed weapons. (Exhibits 17, 18)

11. SPC Olofson has admitted to many soldiers that he is a member of an anti-government militia. (Exhibits 5, 7, 8, 9, 10)

12. Since the investigation began, SPC Olofson has been AWOL from the 2nd Brigade. He has not returned to the unit nor has he returned telephone calls. It can be inferred that he is hiding his misconduct. Since the investigation began, SFC [REDACTED] has refused to answer any questions, even though counsel has been appointed for him. (Exhibit 12)

13. In conclusion, SFC [REDACTED] and SPC Olofson violated 18 USC 1030: Unauthorized Access To A Government Computer, 18 USC 1030: Wrongful Damage Of A Government Computer, 18 USC 371: Conspiracy, the Privacy Act, AR 380-5, AR 380-19, USARC Memorandum 25-70, USARC Memorandum 380-1. Ninety-one soldiers' identities may have been sold or given to persons outside the military. Untold damage was done to the computers, soldiers' private information was accessed, and illegal access by outside organizations was possible. Fortunately, the unit is a T/SSI battalion and does not handle classified information.

SECTION V - RECOMMENDATIONS

1. Request Department Of The Army, United States Army Criminal Investigation Command Computer Crime Investigative Unit, Fort Belvoir, Virginia 22060-5598 to conduct a formal criminal investigation. It is necessary to find out if the 91 identities have been sold to, given to or used by persons outside the military.
2. Mr. [REDACTED] receive a General Officer's letter of reprimand for not performing his duty of supervising [REDACTED] and thus permitting two soldiers to compromise military computing systems and personnel information.
3. These findings should be shared by the approving authority with the Brigade and Battalion commanders. LTC Ricks should consider rescinding SPC Olofson's award. SPC Olofson should be involuntarily separated from the Reserves, and receive a General Officer's letter of reprimand for violating numerous regulations and not informing the command of his civilian convictions. If appropriate, he should also be reduced in grade.
4. SFC [REDACTED] should have his security clearance revoked, and he should be reduced in grade, removed from the AGR system, barred to reenlistment, involuntarily separated and given a General Officer's letter of reprimand. He willingly put his soldiers and command in harm's way.
5. All Battalion personnel should be educated on the cyber security.

NO

NO

Yes

Yes

yes

Consider Bde Counseling Statement  
or Bde Level Letter of Reprimand

with [REDACTED]  
18 Aug 02